REPRODUCTION EQUIPMENT SECURITY CONCERNS

Evolution and technological advances in copier technology have generated non-traditional security concerns associated with the reproduction equipment employed in contractor unclassified and classified work environments. These concerns are primarily categorized as an increased risk of inadvertent disclosure to non-authorized personnel. Similar, and even greater, concerns have arisen about new digital printers/facsimile machines using the same technologies. Digital copiers, printers and/or facsimile machines are Information Systems that require, at the very least, a vulnerability assessment by an Information System Security Manager (ISSM) and possibly an accreditation by DSS before being used to produce or reproduce classified information. Always contact your DSS Industrial Security Representative (IS Rep) and/or Information System Security Professional (ISSP) if there is any doubt.

Image Retention

Older copiers have a problem with image retention on internal drums and platens. Previous countermeasures involved cleaning paper pathways and retaining drums or drum coatings indefinitely. Newer copiers may still have this problem, but normally to a lesser degree. Many new copiers do not have drums but use processes similar to laser printers. Most copiers can be sanitized by running at least one page of full text (font test acceptable) followed by removal of main electrical and any battery power.

Hidden Copies

Many copiers now make hidden copies that are deposited into an internal bin. Service personnel use these copies as a historical reference of copy quality. Copiers with this feature must be sanitized after every use and the internal bin examined or used in an open storage environment. Procedures should be implemented to ensure all classified materials are removed before servicing or between different need to know (NTK) copier sessions.

Internal Hard Drives

The same concerns exist for computer hard drives (i.e., accreditation before classified use). Internal drives require open storage approval and might have to be retained permanently upon equipment removal or maintenance.

Non-volatile memory

The same concerns exist as for computer memory. Sanitization may require overwrite of memory locations or removal/destruction of chips. If non-volatile memory contains “ONLY” machine instructions and can NEVER allow storage of user data, the concern is minimized. Remember, always contact your DSS IS Representative and/or ISSP if there is any doubt.

Remote Maintenance Capability

Several copier models, especially the newer, larger ones, have a feature for remote diagnostics using a built in or external modem. In some cases, the service provider can call in over a telephone line and perform health/welfare checks where in other cases, the copier can call out for maintenance if a problem is detected. Any feature allowing remote access is prohibited.

On-site maintenance

On-site maintenance hazards associated with unavoidable features can be effectively mitigated through traditional sanitizing steps coupled with additional steps to reduce maintenance personnel exposure to the information stored by classified-use copiers. Maintenance personnel not authorized access to the information processed by the copier should be escorted and closely observed by a qualified and cleared individual. On-site maintenance often requires the use of diagnostic or service software resident on a laptop computer or other diagnostic device. Clearing procedures should be used to erase memory buffers and on-board storage devices of potentially classified information. Service personnel computing devices used to perform maintenance require accreditation by DSS before being used by the maintenance service company.

RECOMMENDATION

While almost any copier can be approved for classified use if the correct procedures are followed, it is important that consideration be given to the non-traditional features associated with later model copiers that place information at potential risk of compromise. These features typically involve the internal physical or electronic storage of information processed by machine in a manner exploitable by non-authorized personnel. In classified-use applications, these hazards can be avoided to a great extent through careful equipment selection and attention to feature activation during copier installation and setup. Through the development and implementation of procedures that address the actions and control of on-site maintenance personnel, unavoidable hazards can be mitigated. Procedures must ensure that prior to maintenance all memory buffers and other storage devices within the copier are cleared of classified information. Copier feature availability and implementation vary widely among copier models. As such, this notice provides general information to enhance awareness of the hazard and advocates additional consideration for copier security.

Information regarding the feature set of specific copiers and maintenance procedures should be sought from manufacturers, sales representatives, and maintenance functions and shared with the DSS Industrial Security Representative and/or Information System Security Professional (ISSP).